PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04K 1/00

A1

(11) International Publication Number: **WO 00/45539**

(43) International Publication Date: 3 August 2000 (03.08.00)

(21) International Application Number: PCT/US00/02174

(22) International Filing Date: 28 January 2000 (28.01.00)

(30) Priority Data:

60/117,788	29 January 1999 (29.01.99)	US
60/128,772	9 April 1999 (09.04.99)	US

(71) Applicant *(for all designated States except US)*: GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MEDVINSKY, Sasha [US/US]; 8873 Hampe Court, San Diego, CA 92129 (US). ANDERSON, Steven, E. [US/US]; 5521 Taft Avenue, San Diego, CA 92037 (US). MORONEY, Paul [US/US]; 3411 Western Springs Road, Olivenhain, CA 92024 (US). SPRUNK, Eric [US/US]; 6421 Cayenne Lane, Carlsbad, CA 92009 (US). FELLOWS, Jonathan, A. [US/US]; 13161 Shalimar Place, Del Mar, CA 92014 (US).

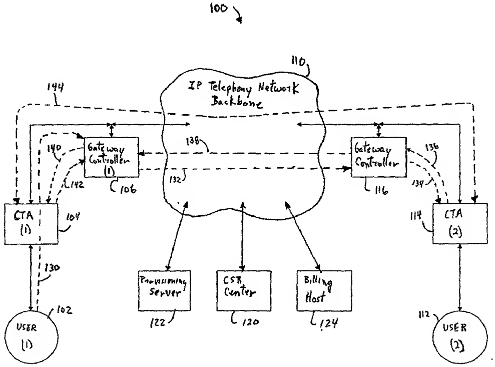
(74) Agents: TAGLIAFERRI, Daniel, D. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: KEY MANAGEMENT FOR TELEPHONE CALLS TO PROTECT SIGNALING AND CALL PACKETS BETWEEN CTA'S

(57) Abstract



A system for establishing a secure communication channel between a first user (102) and a second user (112) in an IP telephony network. The first user and the second user are coupled to first (104) and second (114) telephony adapters, which in turn, are coupled to first (106) and second (116) gateway controllers, respectively, wherein the gateway controllers control user access to the IP telephony network. The telephony adapters are used to encrypt and decrypt user information exchanged over the IP telephony network. The system includes a method which begins when a request is received at the first gateway controller to establish a secure communication channel between the first user and the second user. Next, a secret key (408) is generated at the first gateway controller. A copy of the secret key is distributed to the first and second telephony adapters over previously established secure connections. Finally, the secure communication channel is established (422) between the first user and the second user by encrypting and decrypting information using the secret key.